(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
23 décembre 2004 (23.12.2004)

PCT

(10) Numéro de publication internationale
WO 2004/111831 A2

(51) Classification internationale des brevets[7] : G06F 7/00

(21) Numéro de la demande internationale :
PCT/EP2004/051144

(22) Date de dépôt international : 17 juin 2004 (17.06.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
03/07379 18 juin 2003 (18.06.2003) FR

(71) Déposant *(pour tous les États désignés sauf US)* : GEMPLUS [FR/FR]; Avenue du Pic de Bertagne, Parc d'activité de Gémenos, F-13420 Gemenos (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : JOYE, Marc [BE/FR]; Traverse des Jardins, F-83640 Saint Zacharie (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: METHOD FOR COUNTERMEASURING BY MASKING THE ACCUMULATOR IN AN ELECTRONIC COMPONENT WHILE USING A PUBLIC KEY CRYPTOGRAPHIC ALGORITHM

(54) Titre : PROCEDE DE CONTRE-MESURE PAR MASQUAGE DE L'ACCUMULATEUR DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE PUBLIQUE

(57) Abstract: The invention relates to a method for countermeasuring in an electronic component while using a public key cryptographic algorithm. The invention is characterized in that the method comprises an exponentiation calculation with a left-to-right exponentiation algorithm y=g^d, in which g and y are elements of the specified group G noted in a multiplicative manner and d is a predetermined number. The inventive method is also characterized by comprising a random selection step at the beginning of or during the execution of said exponentiation algorithm in a deterministic or probabilistic manner for masking the accumulator A.

(57) Abrégé : La présente invention concerne un procédé de contremesure dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé publique. Cette invention est remarquable en ce le procédé comprend un calcul d'exponentiation, avec un algorithme d'exponentiation de type gauche-droite, de type y=g^d où g et y sont des éléments du groupe déterminé G noté de façon multiplicative et d est un nombre prédéterminé, ledit procédé étant caractérisé en ce qu'il comprend une étape de tirage aléatoire, au début ou durant l'exécution dudit algorithme d'exponentiation de façon déterministe ou probabiliste, pour masquer l'accumulateur A.

WO 2004/111831 A2